UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/854,525	05/15/2001	Timothy M. Dierks	06944.0035	8225

293 7590 11/04/2004

DOWELL & DOWELL PC
2111 Eisenhower Ave.
Suite 406
Alexandria, VA 22314

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/854,525	DIERKS ET AL.	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 May 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-14 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1, 2, 5, 7, 10, 11, 13 are rejected under 35 U.S.C. 102(b) as being anticipated by Saito.

In reference to claim 1:

Saito discloses a method of controlling access to the data stored on a device, the method comprising the steps of:

- Generating a symmetric key, where the symmetric key is KS1. (Column 6, lines 60-65)
- Encrypting said data by performing a first mathematical operation on said data, said first mathematical operation associated with said symmetric key, where the content data is encrypted using the symmetric key KS1. (Column 7, line 65-Column 8, line 5)

- Intercepting control signals requesting access to said data, where the control signals are intercepted by a processor handle access requests to the data to process the requests. (Column 6, lines 43-47, lines 60-65)
- Decrypting said data by selectively performing a complimentary second mathematical function on said data, said complimentary second mathematical operation associated with said symmetric key, where the content may also be decrypted with the symmetric key KS1. (Column 8, lines 13-18)
- Maintaining data in encrypted form until access thereto is requested, where the content remains encrypted until decrypted. (Column 7, line 65- Column 8, line 5)

In reference to claim 2:

Saito (Column 6, lines 60-65) discloses the method of claim 1, wherein said data includes logically linked data records to form a database.

In reference to claim 5:

Saito discloses a method of securing data on a personalized device comprising the steps of:

- Generating a secure symmetric key, where the secure symmetric key is KS1. (Column 6, lines 60-65)
- Encrypting said data with said secure symmetric key in accordance with the predetermined algorithm, where the data content is encrypted with the secure symmetric key, KS1. (Column 7, line 65- Column 8, line 5)

- Storing said data in encrypted form until a request for read and write access is made, where the data is encrypted form until it is decrypted. (Column 7, line 65-Column 8, line 5)
- Decrypting said data with said secure symmetric key for read and write access, where the data is decrypted using KS1. (Column 8, lines 13-18)
- Encrypting said secure symmetric key with a public key, where the symmetric key KS1, is encrypted with public key KB1. (Column 6, lines 60-65)

In reference to claim 7:

Saito (Column 7, line 65 – Column 8, line 5) discloses the method of claim 6, wherein said predetermined algorithm is selected from a group of mathematical operations, where the predetermined algorithm is a digital watermark algorithm.

In reference to claim 10:

Saito discloses a method of securing stored data on a mobile computing device and controlling access to said stored data by a user, said method comprising the steps of:

- Associating said stored data with a plurality of unique identifiers, where the data is associated with various user data and user identification. (Column 6, lines 48-67)
- Encrypting said stored data by performing a mathematical operation thereon, and maintaining said stored data in encrypted format, where the data is stored in encrypted form until it is decrypted. (Column 7, line 65 – Column 8, line 5)

- Initiating a first call to access said stored data to a processor, said first call including a unique identifier, where the first call to access data involves acquiring the user identification in a request. (Column 6, lines 35-52)
- Intercepting said first call to assess level of privilege associated with said user, where the level of privilege is the question of whether or not the user has authorization to the requested file, causing the user to supply user data. (Column 6, lines 35-52)
- Manipulating said first call in accordance with said level of privilege to generate a second call to said processor, said second call including said unique identifier, where the second call to the processor is the call to the management center to encrypt hash the user data. (Column 6, lines 38-67)
- Communicating second call to said stored data to access said stored data associated with said unique identifier, where the second call stores the data with the associated identifiers as a hash of the identification data with the content. (Column 6, lines 38-67)
- Decrypting said stored data associated with said unique identifier by performing a complimentary mathematical operation to said stored data, said step of decrypting said stored data in accordance with said level of privilege, where the decrypting of the data only comes in accordance with the privilege of access, and henceforth encrypting the data. (Column 7, line 65- Column 8, line 5)
- Communicating said decrypted stored data associated with said unique identifier to said user (Column 8, lines 13-17)

- Encrypting said stored data with said mathematical operation subsequent to access by said user, where subsequent to access, the data is reencrypted. (Column 8, lines 23-27)

In reference to claim 11:

Saito discloses the method of claim 10, wherein the step of controlling access includes steps of:

- A client application retrieving a handle to a record in memory segment via a first call, where the handle is the label of data content M0 in the database of the data management center. (Column 6, lines 35-42)
- Passing the handle to second call to lock said memory segment associated with said locked memory segment, where the second call locks the identification memory segment with the content. (Column 6, lines 52-60)
- The client application reading or writing to the locked memory segment, where the client later reads the memory segment. (Column 8, lines 13-17)
- Passing said handle to third call to unlock the locked memory segment, upon completion of said reading or writing, where the handle of the content is passed to a third call (Second user) to unlock the memory segment (decrypt the digital content) (Column 9, lines 30-37)

In reference to claim 13:

Saito discloses an improved data security system on a portable device, said system having:

- A data storage unit for storing said data, said data having data records and said each of said data records associated with a unique identifier (Column 6, lines 35-43)
- A processor for executing predetermined instructions belonging to a predetermined instruction set, said instruction set associated with access instructions to said records, where a processor is inherent to a computer or digital terminal.
- A patch for preventing execution of received predetermined instructions, and for verifying origin of said received instructions, and for further generating new instructions associated with said received predetermined instructions, upon verification thereof, where the execution is prevented unless the user can offer up information to verify him or herself including a user ID and user email. (Column 6, lines 35-60)
- Whereby a data record is accessed by initiating an instruction with the unique identifier of the data record to be accessed to the processor, said instruction being intercepted and converted into a new instruction by said patch upon verification of origin, where the instruction is received by the data center, and the identifier of the data record is drawn from user in the request for identification. (Column 6, lines 35-52)

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 3 & 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saito and Zank et al., US patent 6,307,955.

6. Claims 6, 8, 9, 12, 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saito.

In reference to claim 3:

Saito fails to disclose the method of claim 1, wherein symmetric key is generated from random data received from recording stylus movements performed by a user.

Saito however does disclose that the user may be requesting the digital content through using a PDA for input. (Column 3, lines 45-51)

Zank et al. discloses a the generation of a signature key from the data received from recording stylus movements performed by a user. (Column 3, lines 5-17)

Zank et al. (Column 2 , lines 8-15) discloses the advantage of using a signature key from data received from a recording stylus movements, is that it can provide authentication to the user while at the same time provide a key that is difficult for anyone else to forge.

It would have been obvious to one of ordinary skill in the art at the time of invention to

use the data received from recording stylus movements performed by a user as a further method of authenticating a user.

In reference to claim 4:

Saito fails to disclose the method of claim 3, wherein said stylus movements form a bit image, said bit image being used in the generation of said symmetric key.

Zank et al. (Figure 4) & (Column 3, lines 5-17) discloses a the generation of a bit image used in the generation of said symmetric key.

In reference to claim 6:

Saito fails to explicitly disclose a method of claim 5, whereby the step of generating a secure symmetric key include a plurality of different degrees of key length, said key length associated with level of security.

The Examiner takes official notice however, that different degrees of key length where the key length is associated with the level of security was well known in the art at the time of invention. The terms, 40-bit encrypted, 56 bit-encryption, 128 bit encryption, are terms that are well known in the art. The more bits per keys, the longer it takes for a brute force method of breaking the encryption. Thus 128 bit encryption is more secure than 40 bit encryption.

It would have been obvious to one of ordinary skill in the art at the time of invention to include a plurality of different degrees of key length, said length associated with level of security in order to conform with the prevalent method of how most if not all symmetric keys are classified by security.

In reference to claim 8:

Saito fails to explicitly discloses the method of claim 7, wherein said mathematical operations are DES, triple-DES, Skipjack, and Rijndael.

The Examiner takes official notice that DES, triple-DES, Skipjack, and Rijndael were all encryption and mathematical algorithms well known in the art. In fact, the acronym DES stands for Digital Encryption Standard.

It would have been obvious to one of ordinary skill in the art at the time of invention to select from the group of mathematical operations including DES, triple-DES, Skipjack, and Rijndael, because these encryption algorithms are well known in the art, and consequently supported by many vendors, allowing for easy purchasing of hardware chips to implement DES, triple-DES, Skipjack, or Rijndael encryption.

Claim 9 is rejected for the same reasons as claim 8. It is known in the art that DES provides a lower level of encryption that triple-DES. Triple-DES was created to allow

DES chips to continue to be used in the face of the weakening DES algorithm due to the increase in computing power.

In reference to claim 12:

Saito fails to discloses the method of claim 11, wherein the step of controlling said access further includes a step of optimizing access to the data records, said step including maintaining an access list of recently accessed pointers and handles.

The Examiner takes official notice that including an access list of recently accessed pointers and handles for optimizing access is a method well known in the art of computer science. Two major concepts taught in operating systems are temporal and spatial locality. Temporal locality is the concept wherein an area of memory that has recently been accessed has a statistically significant chance of being accessed in the near future. Spatial locality indicates that if an area of memory is accessed, there is a statistically significant chance of data in a nearby address to be accessed in the near future. Both methods are exploited for the cache in processors.

It would have been obvious to one of ordinary skill in the art at the time of invention to optimize access using a list of recently accessed pointers and handles in order to reduce the waiting time and memory access time for files requested.

In reference to claim 14:

Saito discloses a method of claim 1, wherein the method further includes the step of synchronizing a database on said device with a database on another device.

The Examiner takes official notice that the synchronization of databases was well known in the art at the time of invention. Database synchronization is important because one desires to avoid inconsistencies, especially of public records. For example, a problem to the status of a file or book will arise, if in one database, the database states the file has been checked out, while another states it hasn't. A synchronization of databases across several systems is used to avoid this. An example of this can be seen in Boothby, US patent 5684990 "Sychronization of Disparate Databases".

It would have been obvious to one of ordinary skill in the art at the time of invention to synchronization databases in order to maintain accurate and consistent records involving the information of users and secret keys in the content distribution system.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers

for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

October 29th, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100